

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION**

ERIC MANDEL, on behalf of himself and
all others similarly situated,

Plaintiff,

v.

BLACKBAUD, INC., a South Carolina
Resident,

Defendant.

Civil Action No. 2:20-cv-03534-RMG

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Eric Mandel, on behalf of himself and all others similarly situated, alleges the following against Defendant Blackbaud, Inc. (“Blackbaud”), based on personal knowledge as to himself and on information and belief as to all other matters based upon, *inter alia*, the investigation conducted by and through his counsel:

SUMMARY OF THE CASE

1. Plaintiff brings this class action against Blackbaud for its failure to properly secure and safeguard personally identifiable information (including, without limitation, names, dates of birth, gender, address, email address, and financial information) (hereinafter “PII”)¹, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class members that the PII stored by Blackbaud had been compromised.

¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver’s license number, financial account number).

2. Blackbaud is a publicly traded company that provides its customers with cloud-based software, services, expertise, and data intelligence. Blackbaud has “millions of users” located in over 100 countries around the world.²

3. Blackbaud’s customers include nonprofits, foundations, corporations, education institutions, healthcare institutions, and the individual change agents who support them.³

4. In the course of doing business with Blackbaud’s customers, individuals such as Plaintiff are regularly required to provide either Blackbaud’s customers or Blackbaud directly with their PII. That PII is then stored on Blackbaud’s cloud.

5. On September 29, 2020, Plaintiff received a letter dated September 14, 2020, from Allina Health notifying him that his PII, which was stored on Blackbaud’s cloud, had been illegally exposed to unauthorized third parties. The notice sent to Plaintiff indicated that Blackbaud discovered a ransomware attack that compromised PII in its custody and care. The notice specifically informed Plaintiff that the information taken included names and addresses, and possibly dates of birth, “dates we cared for the patient identified in the record; the names of doctors who admitted or treated patients; Allina locations visited.”

6. Other hospitals, colleges, universities and non-profit organizations have provided similar notices that their members, customers, and patients had information compromised in the Data Breach.⁴ Other clients of Blackbaud have informed customers that PII including social security numbers may have been removed by the attacker.⁵

² <https://www.blackbaud.com/company> (Last Accessed September 30, 2020).

³ *Id.*

⁴ *See, e.g.,* <https://ago.vermont.gov/blog/2020/08/10/vermont-public-radio-blackbaud-notice-of-data-breach-to-consumers/>; https://buffalonews.com/news/local/local-hospitals-disclose-data-breach-blamed-on-national-software-company/article_61c999de-ed1e-11ea-995b-0799a158eae0.amp.html (Last Accessed September 30, 2020).

7. Blackbaud has indicated that during the period of the Data Breach, a third party was able to view and subsequently remove data, which included Plaintiff's and Class Members' PII, from Blackbaud's system.

8. The PII exposed in the Data Breach included, among other things, individuals' names, addresses, phone numbers, email addresses, dates of birth, financial information, and medical service information, as described above.

9. This Data Breach was a direct result of Blackbaud's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' PII stored in its cloud.

10. Blackbaud disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data and cyber security systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard individual PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and Class Members with prompt and accurate notice of the Data Breach.

11. As a result of Blackbaud's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of thieves. Plaintiff and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves and/or their family members from the adverse ramifications of the Data Breach, and will forever be at a heightened risk of identity theft and fraud.

⁵ <https://oag.ca.gov/system/files/9028629.PDF>, (Last Accessed September 30, 2020).

12. Plaintiff, on behalf of himself and all others similarly situated, alleges claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, declaratory judgment, breach of confidence, invasion of privacy, and violation of South Carolina's Data Breach Security Act, S.C. Code Ann. §§ 39-1-90. Plaintiff seeks to compel Blackbaud to adopt reasonably sufficient security practices to safeguard PII that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future.

JURISDICTION AND VENUE

13. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Blackbaud and is a citizen of a foreign state. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

14. Venue is proper under 28 U.S.C. § 1391(c) because Blackbaud is a corporation that does business in and is subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including the decisions made by Blackbaud's governance and management personnel that led to the breach.

PARTIES

15. Plaintiff Eric Mandel is a resident and citizen of Minnetonka, Minnesota. He was treated at an Allina Health facility in Minnesota.

16. On or about September 29, 2020, Plaintiff received a letter from Allina Health informing him that his PII, which was stored on Blackbaud's cloud in connection with the

fundraising efforts of Allina's 13 "philanthropic foundations," had been illegally exposed to unauthorized third parties. As detailed above, Allina Health advised Plaintiff that as a result of the Data Breach, unauthorized third parties were able to view and remove his PII.

17. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time monitoring various accounts in an effort to detect and prevent any misuses of his PII.

18. Plaintiff has had to, and continues to, spend his valuable time to protect the integrity of his PII—time which he would not have had to expend but for the Data Breach.

19. Plaintiff suffered actual injury from having his PII exposed as a result of the Data Breach including, but not limited to: (a) time spent monitoring accounts for fraudulent activity; (b) damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Allina Health and Blackbaud; (c) imminent and impending injury arising from the increased risk of fraud and identity theft.

20. As a result of the Data Breach, Plaintiff will continue to be at heightened risk for fraud and identity theft, and their attendant damages for years to come.

21. Blackbaud is a corporation organized under the laws of Delaware with a principal place of business at 2000 Daniel Island Drive, Charleston, South Carolina 29492. It is a cloud-based software company that provides services for customers located in many countries around the world.

FACTUAL BACKGROUND

A. The Blackbaud 2020 Data Breach

22. On September 14, 2020, Allina Health wrote a notice letter to Plaintiff stating that Blackbaud, a vendor of Allina Health's family of 13 philanthropic foundations, experienced a

ransomware attack. The notice stated that the Data Breach involved the unauthorized disclosure of Plaintiff's PII.

23. Blackbaud first detected the Data Breach in May of this year. Upon information and belief, the breach originated at a managed hosting (company-run data center) environment for the Raiser's Edge and NetCommunity products that help organizations manage their fund-raising, keeping track of donors and amounts they have contributed over time.

24. Despite learning of the breach in May, it was not until July 16, 2020, that Blackbaud finally notified its customers, like Allina Health and its philanthropic foundations, of the Data Breach. The notice, updated September 29, 2020, states: ⁶

In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. The cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. This incident did not involve solutions in our public cloud environment (Microsoft Azure, Amazon Web Services), nor did it involve the majority of our self-hosted (private cloud) environment. Customers who this applies to who we believe are using these fields for such information were contacted the week of September 27, 2020 and were provided with additional support. We sincerely apologize that this happened and will continue to partner closely with our customers as we jointly navigate this cybercrime incident.

⁶ The notice is available on Blackbaud's website. *See* Learn More About the Ransomware Attack We Recently Stopped, Blackbaud Newsroom (July 16, 2020), <https://www.blackbaud.com/newsroom/article/2020/07/16/learn-more-about-the-ransomware-attack-we-recently-stopped> (last accessed Oct. 6, 2020).

25. According to Blackbaud, between its cybersecurity team, a forensics expert and law enforcement, Blackbaud “successfully prevented the cybercriminal from blocking [its] system access and fully encrypting files; and ultimately expelled [the cybercriminal] from [its] system.” Unfortunately, however, prior to being locked out of the Blackbaud system, this unauthorized third party was able to not only view Plaintiff’s and Class Members’ PII for a three-month period, but also was able to remove a copy of a subset of data from the Blackbaud system. Blackbaud claims that it paid a ransom-to-delete because “protecting [its] customers’ data is [its] top priority.”⁷

26. According to Blackbaud, “the cybercriminal may have accessed some unencrypted fields intended for bank account information, social security numbers, usernames and/or passwords... [t]hese new findings do not apply to all customers who were involved in the incident.”⁸

27. The notices received by Plaintiff and Class Members from Blackbaud’s customers provide a clearer picture as to the types of PII that was disclosed in the Data Breach. In Plaintiff’s notice from Allina Health it states that the information taken included his name and address and may have included his data of birth, dates he was cared for, the names of the doctors who treated him and the Allina locations he visited.

28. Although Blackbaud claims that the unauthorized third party did not access financial information, the notice sent out by at least Vermont Public Radio, another one of Blackbaud’s customers, to its members about the Data Breach expressly indicates otherwise. In

⁷ *Id.*

⁸ *Id.*

the notice letter produced to the Vermont Attorney General's Office regarding the Blackbaud data breach, Vermont Public Radio conveyed the following:

Upon learning of the incident from Blackbaud, we conducted our own investigation of the Blackbaud services we use, and the information provided by Blackbaud to determine what information was involved in the incident. The backup files contained member demographic information, contact information, donation dates and amounts. On July 29, 2020, we determined that the backup files contained an image of a check with your name and account number ending in -XXX.⁹

29. Blackbaud's claim that bank account information was not disclosed during the Data Breach is demonstrably false. An image of a check would, at the very least, contain the check holder's name, address, bank routing number, and account number.

30. Blackbaud communicated to its customers that its basis for concluding that the attacker destroyed the stolen data and has not disseminated the data further is because Blackbaud paid their monetary demands.¹⁰ . Blackbaud cannot reasonably rely on the word of cybercriminals to ensure that this data, which the cybercriminal gained unauthorized access to in the first place, was indeed destroyed, or that prior to destruction, subsequent copies were not made.

31. Blackbaud had an obligation to keep Plaintiff's and Class Members' PII safe from unauthorized disclosure, which it failed to do.

B. Blackbaud Acquires, Collects, and Stores Plaintiff's and Class Members' PII

32. In the ordinary course of doing business with Blackbaud's customers, individuals are regularly required to provide either Blackbaud's customers or Blackbaud directly with

⁹<https://ago.vermont.gov/blog/2020/08/10/vermont-public-radio-blackbaud-notice-of-data-breach-to-consumers/> (Last Accessed September 30, 2020).

¹⁰ <https://www.blackbaud.com/securityincident> (Last Accessed September 30, 2020).

sensitive, personal and private information which is then collected, stored, and maintained by Blackbaud.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Blackbaud assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

34. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and the Class Members relied on Blackbaud to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

35. Blackbaud acknowledges its obligation to maintain the privacy of individual PII entrusted to it. For example, Blackbaud's Privacy Policy North America ("Privacy Policy") states as follows:

At Blackbaud, we are committed to protecting your privacy. This Policy applies to Blackbaud's collection and use of personal data in connection with our marketing and provision of the Blackbaud Solutions, customer support and other services (collectively, the "Services"), for example if you are a customer, visit the website, interact with us at industry conferences, or work for a current or prospective customer of the Services.

If you're a constituent, supporter, patient or student of one of our customers, to which we provide the Services, your data will be used in accordance with that customer's privacy policy. In providing the Services, Blackbaud acts as a service provider and thus, this Policy will not apply to constituents of our customers.¹¹

36. With regard to securing its constituents, supporters, patients or students of one of Blackbaud's customers, Blackbaud further represents with regard to the security of personal information:

¹¹ <https://www.blackbaud.com/company/privacy-policy/north-america> (Last Accessed September 30, 2020).

We restrict access to personal information collected about you at our website to our employees, our affiliates' employees, those who are otherwise specified in this Policy or others who need to know that information to provide the Services to you or in the course of conducting our business operations or activities. While no website can guarantee exhaustive security, we maintain appropriate physical, electronic and procedural safeguards to protect your personal information collected via the website. We protect our databases with various physical, technical and procedural measures and we restrict access to your information by unauthorized persons. We also advise all Blackbaud employees about their responsibility to protect customer data and we provide them with appropriate guidelines for adhering to our company's business ethics standards and confidentiality policies. Inside Blackbaud, data is stored in password-controlled servers with limited access.¹²

37. Blackbaud has made specific commitments regarding the maintenance of student's private information. In April of 2015 with regard to its K-12 school providers, Blackbaud signed a pledge to respect student data privacy to safeguard student information. The Student Privacy Pledge was created to "safeguard student privacy in the collection, maintenance and use of personal information."¹³

38. Blackbaud represented to students and parents of its K-12 school providers that it would, (1) "[m]aintain a comprehensive security program:" and (2) "[b]e transparent about collection and use of student data."¹⁴

39. In further support of this representation and promise to student and parent users, Travis Warrant, president of Blackbaud's K-12 Private Schools Group, stated:

Blackbaud is committed to protecting sensitive student data and security... The Pledge will better inform our customers, service providers and the general public of our dedication to protecting student privacy. The Pledge details ongoing industry practices that meet (and in some cases, exceed) all federal requirements,

¹² <https://www.blackbaud.com/company/privacy-policy/north-america> (Last Accessed September 30, 2020).

¹³ https://www.blackbaud.com/newsroom/article/2015/04/22/blackbaud-signs-pledge-to-respect-student-data-privacy?_ga=2.16964730.2109423225.1601485764-1139314478.1601485764 (Last Accessed September 30, 2020).

¹⁴ *Id.*

and encourages service providers to more clearly articulate their data privacy practices.¹⁵

40. Yet, despite all of this “commitment to protecting privacy,” Blackbaud failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiff’s and Class Members’ PII. Blackbaud had the resources to prevent a breach but neglected to adequately invest in data and cyber security.

C. The Value of Personally Identifiable Information and the Effects of Unauthorized Disclosure

41. The types of information compromised in the Data Breach are highly valuable to identity thieves. Names, email addresses, mailing address, telephone numbers, birthdate, gender, financial information, and other valuable PII can all be used to gain access to a variety of existing accounts and websites and can be used in other ways to effectuate identity theft.

42. Identity thieves can also use the PII to harm Plaintiff and Class Members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver’s licenses, committing insurance fraud, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and

¹⁵ *Id.*

monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.¹⁶

43. To put it into context, the 2013 Norton Report, based on one of the largest consumer cybercrime studies ever conducted, estimated that the global price tag of cybercrime was around \$113 billion at that time, with the average cost per victim being \$298 dollars.

44. The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the PII they have obtained. Indeed, in order to protect themselves, Class Members will need to remain vigilant against unauthorized data use for years and decades to come.

45. Once stolen, PII can be used in a number of different ways. One of the most common is that it is offered for sale on the “dark web,” a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users’ identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and PII.¹⁷ Websites appear and disappear quickly, making it a very dynamic environment.

46. Once someone buys PII, it is then used to gain access to different areas of the victim’s digital life, including bank accounts, social media, and credit card details. During that

¹⁶ The President’s Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, Federal Trade Commission, 11 (April 2007), <https://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf>

¹⁷ Brian Hamrick, *The dark web: A trip into the underbelly of the internet*, WLWT News (Feb. 9, 2017 8:51 PM), <http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-internet/8698419>.

process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

47. Blackbaud is well aware of the profound and widespread impact a data breach to its system can have. In its 2019 Annual Report, Blackbaud acknowledged the dangers:

If the security of our software is breached, we fail to securely collect, store and transmit customer information, or we fail to safeguard confidential donor data, we could be exposed to liability, litigation, penalties and remedial costs and our reputation and business could suffer.

Fundamental to the use of our solutions is the secure collection, storage and transmission of confidential donor and end user data and transaction data, including in our payment services. Despite the network and application security, internal control measures, and physical security procedures we employ to safeguard our systems, we may still be vulnerable to a security breach, intrusion, loss or theft of confidential donor data and transaction data, which may harm our business, reputation and future financial results.

Like many major businesses, we are, from time to time, a target of cyber-attacks and phishing schemes, and we expect these threats to continue. Because of the numerous and evolving cybersecurity threats, including advanced and persistent cyber-attacks, phishing and social engineering schemes, used to obtain unauthorized access, disable or degrade systems have become increasingly more complex and sophisticated and may be difficult to detect for periods of time, we may not anticipate these acts or respond adequately or timely...

Further, the existence of vulnerabilities, even if they do not result in a security breach, may harm client confidence and require substantial resources to address, and we may not be able to discover or remedy such security vulnerabilities before they are exploited, which may harm our business, reputation and future financial results.¹⁸

D. Blackbaud Failed to Comply With FTC Requirements

48. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for

¹⁸ <https://investor.blackbaud.com/static-files/9cd70119-4e13-4d47-b068-3c228c580417> (Last Accessed September 30, 2020).

business highlighting the importance of reasonable data and cyber security practices. According to the FTC, the need for data and cyber security should be factored into all business decision-making.¹⁹

49. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data and cyber security principles and practices for business.²⁰ The guidelines note businesses should protect the personal customer and consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

50. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.²¹

¹⁹ Federal Trade Commission, *Start With Security*, available at <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

²⁰ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>

²¹ FTC, *Start With Security*, *supra* note 19.

51. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer and consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data and cyber security obligations.

52. Blackbaud was at all times fully aware of its obligation to protect the personal and financial data of its customers. Blackbaud was also aware of the significant repercussions if it failed to do so.

53. Blackbaud’s failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

E. The Blackbaud Data Breach Caused Harm and Will Result in Additional Fraud

54. The ramifications of Blackbaud’s failure to keep Plaintiff’s and Class Members’ data secure are long lasting and severe.

55. Consumer victims of data breaches are much more likely to become victim of identity fraud. This conclusion is based on an analysis of four years of data that correlated each year’s data breach victims with those who also reported being victims of identity fraud.²²

56. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”²³ The FTC describes “identifying

²² 2014 LexisNexis True Cost of Fraud Study, <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf>.

²³ 17 C.F.R. § 248.201 (2013).

information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.”²⁴

57. PII is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, “they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance.”²⁵

58. Identity thieves can use personal information, such as that of Plaintiff and Class Members, which Blackbaud failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver’s license or identification card in the victim’s name but with another’s picture; using the victim’s information to obtain government benefits; or filing a fraudulent tax return using the victim’s information to obtain a fraudulent refund.

59. Javelin Strategy and Research reports that identity thieves have stolen \$112 billion in the past six years.²⁶

60. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice’s Bureau of Justice Statistics (“BJS”) found that identity theft victims “reported spending

²⁴ *Id.*

²⁵ Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft>.

²⁶ <https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point>

an average of about 7 hours clearing up the issues” and resolving the consequences of fraud in 2014.²⁷

61. An independent financial services industry research study conducted for BillGuard—a private enterprise that automates the consumer task of finding unauthorized transactions that might otherwise go undetected—calculated the average per-consumer cost of all unauthorized transactions at roughly US \$215 per cardholder incurring these charges,²⁸ some portion of which could go undetected and thus must be paid entirely out-of-pocket by consumer victims of account or identity misuse.

62. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁹

63. Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

F. Plaintiff and Class Members Suffered Damages

²⁷ Victims of Identity Theft, 2014 (Sept. 2015) available at: <http://www.bjs.gov/content/pub/pdf/vit14.pdf>.

²⁸ Hadley Malcom, *Consumers rack up \$14.3 billion in gray charges, research study commissioned for Billguard by Aite Research, USA Today* (July 25, 2013), available at: <https://www.usatoday.com/story/money/personalfinance/2013/07/25/consumers-unwanted-charges-in-billions/2568645/>.

²⁹ GAO, Report to Congressional Requesters, at 29 (June 2007), <http://www.gao.gov/new.items/d07737.pdf>

64. The PII of Plaintiff and Class Members is private and sensitive in nature and was left inadequately protected by Blackbaud. Blackbaud did not obtain Plaintiff's and Class Members' consent to disclose their PII to any other person as required by applicable law and industry standards.

65. The Data Breach was a direct and proximate result of Blackbaud's failure to properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Blackbaud's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

66. Blackbaud had the resources to prevent a breach. In 2019, Blackbaud reported that it had 45,000 customers located in over 100 countries, with a total addressable market greater than \$10 billion.³⁰

67. Had Blackbaud remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Blackbaud would have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

68. As a direct and proximate result of Blackbaud's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring

³⁰ <https://investor.blackbaud.com/static-files/9cd70119-4e13-4d47-b068-3c228c580417> (Last Accessed August 30, 2020).

them to purchase credit monitoring services and take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

69. Blackbaud’s wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff’s and Class Members’ PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. monies paid for credit monitoring and identity theft prevention services;
- b. theft of their personal and financial information;
- c. the imminent and certainly impending injury flowing from potential fraud and identity theft;
- d. the untimely and inadequate notification of the Data Breach;
- e. the improper disclosure of their PII;
- f. loss of privacy;
- g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;
- h. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

- i. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach.

70. While Plaintiff's and Class Members' PII have been compromised, Blackbaud continues to hold consumers' PII, including Plaintiff's and Class Members'. Particularly because Blackbaud has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class Members have an undeniable interest in ensuring that their and PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

71. Plaintiff seeks relief on behalf of himself and as a representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3), and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

All persons whose PII was exposed to unauthorized third parties as a result of the Data Breach on Blackbaud's network ("Nationwide Class").

72. Excluded from the Class are Blackbaud and any entities in which Blackbaud or its subsidiaries or affiliates have a controlling interest, and Blackbaud's officers, agents, and employees. Also excluded from the Class are the judge assigned to this action, members of the judge's staff, and any member of the judge's immediate family.

73. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

74. **Numerosity:** The members of each Class are so numerous that joinder of all members of any Class would be impracticable. While the exact number of individuals affected in

the Data Breach is unknown, upon information and belief, it is well in excess of a hundred, and therefore meets the numerosity requirement of 23(a)(1).

75. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class Members, including:

- a. Whether Blackbaud represented to the Class that it would safeguard Class Members' PII;
- b. Whether Blackbaud owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- c. Whether Blackbaud breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- d. Whether Class Members' PII was accessed, compromised, or stolen in the Data Breach;
- e. Whether (and when) Blackbaud knew about any security vulnerabilities that led to the Data Breach before it was announced to the public and whether Blackbaud failed to timely notify the public of those vulnerabilities and the Data Breach;
- f. Whether Blackbaud knew about the Data Breach before it was announced to the public and Blackbaud failed to timely notify the public of the Data Breach;
- g. Whether Blackbaud's representations that it would secure and protect the PII of Plaintiff and members of the class were facts that reasonable persons could be expected to rely upon when deciding whether to use Blackbaud's services;

- h. Whether Blackbaud misrepresented the safety of its many systems and services, specifically the security thereof, and its ability to safely store Plaintiff's and Class Members' PII;
- i. Whether Blackbaud concealed crucial information about its inadequate data and cyber security measures from Plaintiff and the Class;
- j. Whether Blackbaud failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data and cyber security;
- k. Whether Blackbaud knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' PII secure and prevent the loss or misuse of that information;
- l. Whether such representations were false with regard to storing and safeguarding Plaintiff's and Class Members' PII;
- m. Whether such representations were material with regard to storing and safeguarding Class Members' PII;
- n. Whether Blackbaud's conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, et seq.;
- o. Whether Plaintiff and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and
- p. Whether Plaintiff and the other Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

76. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

77. **Typicality:** Plaintiff's claims are typical of the claims of the other members of their respective classes because, among other things, Plaintiff's and the other Class Members were injured through the substantially uniform misconduct by Blackbaud. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. Plaintiff's claims and those of other Class Members arise from the same operative facts and are based on the same legal theories.

78. **Adequacy of Representation:** Plaintiff is an adequate representative of the class because his interests do not conflict with the interests of the other Class members he seeks to represent; he has retained counsel competent and experienced in complex class action litigation and Plaintiff will prosecute this action vigorously. The Class Members' interests will be fairly and adequately protected by Plaintiff and his counsel.

79. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Blackbaud, making it impracticable for Class Members to individually seek redress for Blackbaud's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

80. Further, Blackbaud has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

81. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Class Members' PII was accessed, compromised, or stolen in the Data Breach;
- b. Whether (and when) Blackbaud knew about any security vulnerabilities that led to the Data Breach before it was announced to the public and whether Blackbaud failed to timely notify the public of those vulnerabilities and the Data Breach;
- c. Whether Blackbaud's representations that it would secure and protect the PII of Plaintiff and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Blackbaud's services;
- d. Whether Blackbaud misrepresented the safety of its many systems and services, specifically the security thereof, and its ability to safely store Plaintiff's and Class Members' PII;
- e. Whether Blackbaud concealed crucial information about its inadequate data and cyber security measures from Plaintiff and the Class;
- f. Whether Blackbaud failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data and cyber security;

- g. Whether Blackbaud knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' PII secure and prevent the loss or misuse of that information;
- h. Whether Blackbaud failed to "implement and maintain reasonable security procedures and practices" for Plaintiff's and Class Members' PII in violation of Section 5 of the FTC Act;
- i. Whether Blackbaud failed to provide timely notice of the Data Breach;
- j. Whether Blackbaud owed a duty to Plaintiff and the Class to safeguard their PII and to implement adequate data and cyber security measures;
- k. Whether Blackbaud breached that duty;
- l. Whether such representations were false with regard to storing and safeguarding Plaintiff's and Class Members' PII; and
- m. Whether such representations were material with regard to storing and safeguarding Class Members' PII.

FIRST CAUSE OF ACTION

Negligence

(On behalf of Plaintiff and the Nationwide Class)

82. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

83. Blackbaud owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Blackbaud's data security systems to ensure that Plaintiff's and Class Members' PII in Blackbaud's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its data systems in a timely

manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data and cyber security measures consistent with industry standards.

84. Blackbaud knew that the PII belonging to Plaintiff and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Blackbaud also knew of the serious harms that could happen if the PII of Plaintiff and the Class was wrongfully disclosed, that disclosure was not fixed, or Plaintiff and the Class were not told about the disclosure in a timely manner.

85. Blackbaud had a common law duty to prevent foreseeable harm to those whose PII it stored on its cloud. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Blackbaud knew that it was more likely than not Plaintiff and other Class Members would be harmed.

86. Blackbaud is morally culpable, given the prominence and potential of security breaches in the software industry and its own recent massive breach which demonstrated Blackbaud's wholly inadequate cyber security measures and safeguards.

87. Blackbaud breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite repeated failures and intrusions, and allowing unauthorized access to Plaintiff's and the other Class member's PII.

88. Blackbaud breached the duties it owed to Plaintiff and Class Members described above and thus was negligent. Blackbaud breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose in a timely fashion that Plaintiff's and Class Members' PII in Blackbaud's possession had been or was reasonably believed to have been, stolen or compromised.

89. Blackbaud's failure to comply with industry and federal regulations further evidences Blackbaud's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' PII.

90. Blackbaud's breaches of these duties were not merely isolated incidents or small mishaps. Rather, the breaches of the duties set forth above resulted from a long-term company-wide refusal by Blackbaud to acknowledge and correct serious and ongoing data and cyber security problems.

91. But for Blackbaud's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised, stolen, and viewed by unauthorized persons. Blackbaud's negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Class and all resulting damages.

92. Blackbaud also had a duty to safeguard the PII of Plaintiff and Class Members and to promptly notify them of a breach because of laws and regulations that require Blackbaud to reasonably safeguard PII, as detailed herein.

93. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their credit

profiles, monitor their health insurance and health care provider accounts and profiles, cancel current passports and obtain new passports, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Blackbaud's misconduct.

94. The injury and harm suffered by Plaintiff and the Class Members was the reasonably foreseeable result of Blackbaud's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII. Blackbaud knew its systems and technologies for processing and securing the PII of Plaintiff and the Class had numerous security vulnerabilities.

95. As a result of this misconduct by Blackbaud, the PII of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiff and Class Members also suffered diminution in value of their PII in that it is now easily available to hackers on the dark web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

SECOND CAUSE OF ACTION

Negligence Per Se

(On behalf of Plaintiff and the Nationwide Class)

96. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

97. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Blackbaud, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Blackbaud’s duty in this regard.

98. Blackbaud violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Blackbaud’s conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach with a cloud-based company as large as Blackbaud, including, specifically, the immense damages that would result to Plaintiff and Class Members.

99. Blackbaud’s violation of Section 5 of the FTC Act constitutes negligence *per se*.

100. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

101. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data and cyber security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

102. As a direct and proximate result of Blackbaud’s negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing “freezes” and “alerts” with credit reporting

agencies, monitoring health insurance and health care provider accounts and files, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

103. Additionally, as a direct and proximate result of Blackbaud's negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Blackbaud's possession and is subject to further unauthorized disclosures so long as Blackbaud fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

104. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

105. Plaintiff and Class Members were required to provide PII, including names, addresses, dates of birth, and various financial information to Blackbaud and Blackbaud's customers in exchange for Blackbaud and Blackbaud's customers' services.

106. Blackbaud solicited and invited Plaintiff and Class Members to provide their PII as part of Blackbaud's regular business practices. Plaintiff and Class Members accepted Blackbaud's offers and provided PII to Blackbaud.

107. As part of these transactions, Blackbaud agreed to safeguard and protect the PII of Plaintiff and Class Members.

108. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Blackbaud's data and cyber security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class Members believed that Blackbaud would use part of the monies paid to Blackbaud either by them directly or through Blackbaud's customers, to fund adequate and reasonable data and cyber security practices.

109. Plaintiff and Class Members would not have provided and entrusted PII to Blackbaud or Blackbaud's customers or would have paid less for Blackbaud's services in the absence of the implied contract or implied terms between them and Blackbaud. The safeguarding of the PII of Plaintiff and Class Members was critical to realize the intent of the parties.

110. Plaintiff and Class Members fully performed their obligations under the implied contracts with Blackbaud.

111. Blackbaud breached its implied contracts with Plaintiff and Class Members to protect PII in its possession when it: (1) failed to have security protocols and measures in place to protect that information; and (2) disclosed that information to unauthorized third parties.

112. As a direct and proximate result of Blackbaud's breaches of implied contract, Plaintiff and Class Members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

113. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

114. Plaintiff and Class Members have an interest, both equitable and legal, in the PII conferred upon, collected by, and maintained by Blackbaud and that was stolen in the Data Breach.

115. Blackbaud benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Blackbaud understood this benefit.

116. Blackbaud also understood and appreciated that the PII it collected and stored was private and confidential, and its value depended upon Blackbaud maintaining the privacy and confidentiality of that PII.

117. But for Blackbaud's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and entrusted with Blackbaud. Indeed, if Blackbaud had informed Plaintiff and Class Members that Blackbaud's data and cyber security measures were inadequate, Blackbaud would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

118. As a result of Blackbaud's wrongful conduct, Blackbaud has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members. Blackbaud continues to benefit and profit from its retention and use of the PII while its value to Plaintiff and Class Members has been diminished.

119. Blackbaud's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this Complaint, including compiling, using, and retaining Plaintiff's and Class Members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

120. Under the common law doctrine of unjust enrichment, it is inequitable for Blackbaud to be permitted to retain the benefits it received, and still receives, without

justification, from Plaintiff and Class Members in an unfair and unconscionable manner. Blackbaud's retention of such benefits under the circumstances makes it inequitable, constituting unjust enrichment.

121. The benefit conferred upon, received, and enjoyed by Blackbaud was not conferred officiously or gratuitously, and it would be inequitable and unjust for Blackbaud to retain that benefit.

122. Blackbaud is therefore liable to Plaintiff and Class Members for restitution in the amount of the benefit conferred on Blackbaud as a result of its wrongful conduct, including specifically the value to Blackbaud of the PII that was stolen in the Data Breach and the profits Blackbaud is receiving from the use of that PII.

FIFTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Nationwide Class)

123. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

124. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. This Court has broad authority to restrain acts, such as those alleged herein, which are tortious and violate the terms of the laws described above and herein.

125. An actual controversy has arisen in the wake of the Data Breach regarding present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' PII and whether Blackbaud is currently maintaining data and cyber security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise the PII they shared with Blackbaud. Plaintiff alleges that Blackbaud's data and cyber security measures remain inadequate, and that Plaintiff and Class Members continue to suffer injury as a

result of the Data Breach. Plaintiff and Class Members remain at imminent risk that further compromises of the PII provided to Blackbaud will occur in the future.

126. Pursuant to the Court's authority under the Declaratory Judgment Act, the Court should enter a judgment declaring, *inter alia*, the following:

- a. Blackbaud continues to owe a legal duty to secure consumers' PII;
- b. Blackbaud continues to owe a legal duty to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and respective state statutes;
- c. Blackbaud continues to breach these legal duties by failing to employ reasonable measures to secure consumers' PII.

127. The Court should also issue corresponding prospective injunctive relief requiring Blackbaud to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

128. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack any adequate legal remedy, should another data breach occur due to Blackbaud's insufficient practices. As described above, a subsequent data breach is real, immediate, and substantial, as Blackbaud remains a rich target for hackers and other malicious actors. If another data breach occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

129. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Blackbaud if an injunction is issued. Among other things, Plaintiff would be subjected to fraud, identity theft, and other harms should another data breach occur.

The cost to Blackbaud of complying with such an injunction is relatively minimal, and Blackbaud has pre-existing legal obligations to employ such measures.

130. Issuance of the requested injunction will not disserve the public interest. Instead, such an injunction would *benefit* the public by mitigating and preventing another data breach, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and other consumers whose PII would be further compromised.

SIXTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class)

131. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

132. At all times during Plaintiff's and Class Members' interactions with Blackbaud, Blackbaud was fully aware of the confidential and sensitive nature of the PII that Plaintiff and Class Members provided to Blackbaud.

133. As alleged herein and above, Blackbaud's relationship with Plaintiff and Class Members was governed by expectations that PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

134. Plaintiff and Class Members provided PII to Blackbaud with the explicit and implicit understandings that Blackbaud would protect and not permit the PII to be disseminated to any unauthorized parties.

135. Plaintiff and Class Members also provided PII to Blackbaud with the explicit and implicit understanding that Blackbaud would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of information security practices.

136. Blackbaud voluntarily received in confidence Plaintiff's and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

137. Due to Blackbaud's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class Members' PII, that PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

138. As a direct and proximate cause of Blackbaud's actions and/or omissions, Plaintiff and Class Members have suffered damages.

139. But for Blackbaud's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Blackbaud's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

140. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Blackbaud's unauthorized disclosure of PII. Blackbaud knew its computer systems and cyber security practices for accepting and securing Plaintiff's and Class Members' PII had numerous security vulnerabilities because Blackbaud failed to observe industry standard information security practices.

141. As a direct and proximate result of Blackbaud's breaches of confidence, Plaintiff and Class Members have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit

reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

142. As a direct and proximate result of Blackbaud's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SEVENTH CAUSE OF ACTION
Violation of the South Carolina Data Breach Security Act
S.C. Code Ann. §§ 39-1-90
(On Behalf of Plaintiff and the Nationwide Class)

143. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

144. The South Carolina Data Breach Security Act (the "Act") requires persons conducting business in this State and owning, licensing or maintaining computerized data that includes personal identifying information to disclose breaches of the security of the system to those affected. This required disclosure "must be made in the most expedient time possible and without reasonable delay" S.C. Code Ann. § 39-1-90(A).

145. Blackbaud is a "person" as defined by the statute. S.C. Code Ann. § 39-1-90(D)(2).

146. As described more fully above, Blackbaud conducts business in this State and owns, licenses or maintains computerized data that includes personal identifying information.

147. Plaintiff's and Class Members' PII compromised in the Data Breach meets the definition of "personal identifying information" in the statute. S.C. Code Ann. § 39-1-90(D)(3).

148. The Data Breach meets the definition of "Breach of the security of the system" in the statute. S.C. Code Ann. § 39-1-90(D)(1).

149. Blackbaud violated the Act by unreasonably delaying disclosure of the Data Breach to Plaintiff and Class Members whose PII was, or was reasonably believed to have been, acquired by an unauthorized third person.

150. Blackbaud knew or should have known that it was violating South Carolina law by unreasonably delaying disclosure of the Data Breach. This renders Blackbaud's violation of the Act willful and knowing.

151. Upon information and belief, no law enforcement agency determined that notification to Plaintiff and Class Members would impede a criminal investigation.

152. As a result of Defendant's violation of the Act, Plaintiff and Class Members suffered and will continue to suffer damages and injury set forth above.

153. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, attorneys' fees, and any other relief that is just and proper.

EIGHTH CAUSE OF ACTION
Invasion of Privacy – Wrongful Publicizing of Private Affairs
and Wrongful Intrusion Into Private Affairs
(On Behalf of Plaintiff and the Nationwide Class)

154. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

155. Plaintiff and Class Members have a legally protected privacy interest in the PII that is held by Blackbaud, and they are entitled to the protection of their PII against unauthorized access.

156. Plaintiff and Class Members reasonably expected that Blackbaud would protect and secure their PII from unauthorized parties and that their PII would not be disclosed to any unauthorized parties or for any improper purpose.

157. Blackbaud unlawfully invaded the privacy rights of Plaintiff and Class Members by engaging in the conduct described above, including by failing to protect their PII, by publicizing their PII to unauthorized third parties and by unreasonably and intentionally delaying disclosure of the Data Breach.

158. This invasion of privacy resulted from Blackbaud's intentionally publicizing or causing the publication of Plaintiff's and Class Members' PII. This invasion of privacy also resulted from Blackbaud's intentionally intruding upon or causing the intrusion upon the PII.

159. Plaintiff's and Class Members' PII is the type of sensitive, personal information that one normally expects will be from exposure, and the public has no legitimate concern in Plaintiffs' and Class Members' PII.

160. Blackbaud's disclosure of Plaintiff's and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

161. Blackbaud's intentional conduct in disclosing Plaintiff's and Class Members' sensitive, personal information and delaying notification of the disclosure is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

162. The disclosure of Plaintiff's and Class Members' PII was without their consent.

163. As a result of the invasion of privacy caused by Blackbaud, Plaintiff and Class Members suffered and will continue to suffer damages and injury set forth above, including serious mental injury, shame or humiliation.

164. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and on behalf of the other Class Members, respectfully requests this Court enter the following:

- a. An Order certifying this case as a class action;
- b. An Order appointing Plaintiff as class representative;
- c. An Order appointing undersigned counsel as class counsel;
- d. A mandatory injunction directing Blackbaud to hereinafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;
- e. An award of damages, at a minimum, nominal damages;
- f. An award of costs and expenses;
- g. An award of attorneys' fees; and
- h. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims so triable.

Respectfully Submitted,

Dated: October 6, 2020

/s/Frank B. Ulmer

Frank B. Ulmer (Federal ID No. 11071)
Stuart H. McCluer (Federal ID No. 13213)
MCCULLEY MCCLUER PLLC
701 E. Bay St., Suite 411
Charleston, SC 29403
Telephone: (843) 444-5404
Facsimile: (843) 444-5408
Email: fulmer@mcculleymccluer.com
smccluer@mcculleymccluer.com

Counsel for Plaintiff and the Proposed Class

Karen Hanson Riebel, *Pro Hac Vice* forthcoming
Kate M. Baxter-Kauf, *Pro Hac Vice* forthcoming
Maureen Kane Berg, *Pro Hac Vice* forthcoming
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
Email: khriebel@locklaw.com
kmbaxter-kauf@locklaw.com
mkberg@locklaw.com

Counsel for Plaintiff and the Proposed Class

Andrew N. Friedman, *Pro Hac Vice* forthcoming
Victoria S. Nugent, *Pro Hac Vice* forthcoming
Douglas J. McNamara, *Pro Hac Vice* forthcoming
Paul Stephan, *Pro Hac Vice* forthcoming
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue NW
East Tower, 5th Floor
Washington, DC 20005
Telephone: (202) 408-4600
Email: afriedman@cohenmilstein.com
vnugent@cohenmilstein.com
dmcnamara@cohenmilstein.com
pstephan@cohenmilstein.com

Counsel for Plaintiff and the Proposed Class